Math.
No. 128
www.sugakukobo.com

会報 2019 年 1 月
数学工房

2019 年 春 巻 頭 言

今年も数学工房をよろしくお願いいたします。

恒例のお正月の懇親会は、諏訪先生のお年玉講義「数学の楽しみ方～Fibonacci 数列を例として」からはじまりました。内容は、線形漸化式のいくつかの解法の比較から始まり Lucas 数列の周期性についての、Lucas 自身の仕事の紹介、そして Lucas 数列の加除性を、Grothendiek の group scheme の理論を用いて幾何学的な言葉で捉える可能性への気づきから、ご自身の論文に至った経緯に触れられ、最後に桑野道場に出題された不定方程式の問題の会員の熊野充博さんの解答についてのコメントを通じて群論的（幾何学的）観点の重要さ、日々の様々な数学的気づきの大切さを強調されて 6 つの情景からなる数学の学びへの示唆に富む庭園巡りを、おえられました。

このお話は数学工房での学びをどの様にすれば、挫折せずに、楽しめ、意義のあるものにできるのか。会員への応援歌です。この場を借りて諏訪先生には感謝いたします。学びへの示唆と励ましにとんだお話。本当にありがとうございました。なおこの講義のレジュメは HP で公開の予定です。興味のある方は是非ともご覧ください。

数学工房では、抽象線形代数と一般位相の学びを基盤にして各種講座の教程を組立ています。このような理論達で養った抽象力（本質を取り出す能力）を様々なレベルの数学的現象の中で楽しみつつ使えることが学びを生かす、コツです。そしてたくさんの気づきを蓄積していくこと、それは研究レベルの数学にもつながっていくこともあり得るわけです。

2019 年新春 数学工房　桑野耕一

春 学 期 講 座 案 内

2019 年 1 月～4 月

2019 年春学期講座は、入門 2 講座、初級入門 2 講座、初級 3 講座、中級 3 講座を開講します。

<< 春学期講座一覧 >>

略号	講座名	講座開始日	レベル
I.A	解析教程	1 月 20 日	入門
I.B	Residue Calculus	1 月 27 日	初級入門
I.C	Unitary 表現	3 月 16 日	初級
I.F	数学の基本語彙と文法	1 月 19 日	入門
E.A	一様構造　関数空間におけるコンパクト	1 月 26 日	初級
E.C	多様体の基礎理論	1 月 20 日	初級
G	抽象線型代数 Ⅲ	1 月 27 日	初級入門
M.A	Banach 環 Ⅱ	3 月 10 日	中級
M.B	Von Neumann 環	2 月 2 日	中級
M.C	開集合上の超関数	3 月 17 日	中級

IA、IF、G、MB は変則日程となっております。ご注意ください。

◆ I.A　解析教程
＜0＞　Introduction
（0）Fourier 級数の基礎概念
（1）部分和・Dirichlet 核
（2）平均収束・Fejer の定理
（3）実表現との関係
＜1＞ Weyl の一様分布定理
＜2＞ 各点収束についての基礎判定法
＜3＞ Fourier 級数の幾何・核関数・完全正規直交系
＜4＞　直交多項式の Fourier 級数
1/20 より 6 回変則日程 (1/20, 2/3, 2/17, 3/10, 3/24, 4/7)

◆ I.B　Residue Calculus
＜0＞　Introduction
＜1＞　基本的な考え方
（1）Improper Integral
（2）三角関数の定積分

（3）数直線上の積分
（4）特別なタイプの積分
＜2＞　定積分の計算
＜3＞　トピックス
　1/27 より隔週 3 回

◆ I.C　Unitary 表現
＜0＞　Unitary 表現の概念と基本問題
＜1＞　Compact 群の Unitary 表現
（1）Hilbert 直和
（2）Unitary 表現の直和分解
（3）Cyclic 表現
（4）Hilbert-Schmidt の定理
（5）Shur の補題
（6）行列成分
（7）Peter-Weyl の定理
（8）指標
　3/16 より隔週 3 回

◆ I.F　数学の基本語彙と文法 II　無限の作法
＜1＞　準備
（1）Zorn の補題
（2）選択公理
＜2＞　集合の濃度
（1）集合の対等
（2）集合の濃度
＜3＞　トピックス
　2 回変則日程 (1/19, 2/11)

◆ E.A　一様構造　関数空間におけるコンパクト
＜0＞　Introduction
＜1＞　同程度連続性
（1）連続関数の空間　まとめ
（2）同程度連続な一様連続写像族の基本定理
（3）Ascoli-Arzela の定理
（4）いくつかの応用
＜2＞　一様構造
　1/26 より隔週全 3 回

◆ E.C　多様体の基礎理論
＜0＞　Introduction
（1）多元環上の交換子環
（2）ベクトル場の交換子積
（3）Lie 環
＜1＞　ベクトル場の Lie 環
＜2＞　ベクトル場上の 1-パラメータ群
＜3＞　Riemann 多様体の無限小運動
＜4＞　パラコンパクト多様体
　1/20 より隔週全 3 回

◆ G　抽象線型代数 III　内積空間の幾何と作用素のクラス
＜0＞　内積空間
（1）定義と例
（2）内積の基本的な性質
＜1＞　内積空間の幾何
（1）直交系・正規直交系
（2）正射影定理と Cauchy-Schwartz の不等式
（3）正規直交基底の存在・Gram-Schmidt の直交化・Gram 行列
（4）線型形式の表現定理
＜2＞　内積空間の作用素
（1）一般論 Adjoint 定義と諸性質
（2）作用素ノルム
（3）対称変換
　1/27 より 6 回変則日程 (1/27, 2/10, 2/24, 3/17, 3/31, 4/14)

◆ M.A　Banach 環 II　Gelfond の定理
＜1＞　Maximal Ideal 空間
＜2＞　Banach 環の Gelfond 表現
＜3＞　基本的な例
＜4＞　Banach 環と正の汎関数
　3/10 より 3 回変則日程 (2/2, 2/16, 3/9)

◆ M.B　Von Neumann 環　弱位相　σ 弱位相　強位相　Kapalensky の定理
＜1＞　Von Neumann 環の Pre-dual
＜2＞　Kapalensky の定理
＜3＞　可換　Von Neumann 環
　2/2 より 3 回変則日程 (2/2, 2/16, 3/9)

◆ M.C　開集合上の超関数
＜1＞　Schwartz の核定理
＜2＞　擬微分作用素
＜3＞　超関数の合成積
　教科書 142p〜162p をやります。開集合上の超関数の終わりも見えてきました。続編は超関数の応用として Soborev 空間を考えています。
　3/17 より隔週全 3 回

[料金]
通常講座
一括払い ￥32,000（学割￥25,000）
各回払い 3 回のセミナー　1、2 回目￥12,000（学割￥9,000）　3 回目￥10,000（学割￥9,000）
6 回のセミナー　1 回目￥6,500（学割￥6,000）　2 回目以降￥5,500（学割￥4,000）

数学の楽しみ方～ Fibonacci 数列を題材にして

先日の 1 月 13 日に中央大学理工学部数学科の諏訪紀幸先生による「数学の楽しみ方～Fibonacci 数列を題材にして」というタイトルで特別講義が数学工房駒込教室で開催されました。また、特別講義のあとは諏訪先生、桑野先生、および講義の参加者を交えた懇親会が催されました。今回は、いつもの「会員からのメッセージ」に代わり、特別講義と懇親会の様子について、会報編集委員の増田がご報告します。

■藩札学位？！

講義の冒頭、諏訪先生から「藩札学位について知っていますか？」という問いが投げかけられました。藩札学位とは、その藩でしか通用しない学位のことです。桑野先生が以前、会報の巻頭言で、表面的な知識の習得にとどまって、理論を通して身に着けるべき基本技術や方法を自分のものにしていない人が多い、と指摘したことを取り上げて、諏訪先生は大学でもこの藩札学位が横行していると嘆いておられました。

思わず、自分はどうだったかと顧みてみました。私は大学院で制御工学を専攻し、数学関連の論文を読んでいました。工学部出身の私には数学の基礎的な知識が乏しかったこともあり、論文を読んでも頭の中に何も残りませんでした。結局、本質的なことは何も理解しないまま、シミュレーションで何とか修論の体裁を取り繕って卒業しました。私もまさに藩札学位を取得した一人だなあ、と講義の冒頭から耳の痛い思いをしました。

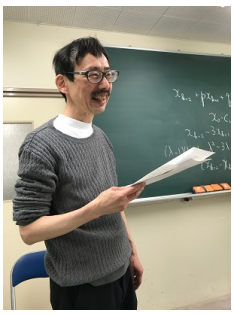

写真 1：諏訪紀幸先生

■講義の内容

講義の内容についてですが、初めに二階線型差分方程式 $a_{k+2}+pa_{k+1}+qa_k=0$ のいろいろな解法を示されました。高校数学では、漸化式と言われているもので、特性方程式 $\lambda^2+p\lambda+q=0$ の 2 つの解 α,β を使用して一般項を求める解法を覚えている人も多いと思います。私は高校時代にこの解き方を習ったとき、方法論としては理解できるものの、なぜ特性方程式の解を使えば数列の一般項を求めることができるのか、その本質を理解できませんでした。

諏訪先生は 2 つ目の解法で、二階線型差分方程式を

$$\begin{cases} x_{k+1}=y_k \\ y_{k+1}=-px_k-qy_k \end{cases}$$

と書き換えたうえで、

$$A=\begin{pmatrix} 0 & 1 \\ -q & -p \end{pmatrix}$$

とおくと、

$$\begin{pmatrix} x_{k+1} \\ y_{k+1} \end{pmatrix}=A\begin{pmatrix} x_k \\ y_k \end{pmatrix}$$

となり、数列の添え字のシフトが実は線型変換であることを示されました。そして、前出の特性方程式の解というのは、この線型変換の固有値になるのです。高校数学の漸化式の問題が、実は線型代数の理論と深く結びついていることがわかります。どうりで高校時代には理解できなかったはずだと納得した次第です。

さらに、諏訪先生は母関数を使った解法も示されました。これは数列 $\{a_k\}_{k\geq 0}$ を形式べき級数の係数とするものです。この解法は私は全く知らなかったもので、これも目から鱗が落ちるような思いでした。

次に類似の問題として、二階線型微分方程式 $\frac{d^2x}{dt^2}+p\frac{dx}{dt}+qx=0$ の解法を示されました。この問題も特性方程式の 2 つの解を使って一般解を求めることができます。したがって、前出の二階線型差分方程式と共通の構造を持っていることがわかります。

以上のように諏訪先生は、いろいろな解法を楽しむことと類似の問題を楽しむことで、数学を表面的にではなく、より深く理解できることを教えてくれました。ちなみに、ピタゴラスの定理の証明法は、知られているだけで 40～50 通りあるそうです。いろいろな証明法にチャレンジしてみるのも面白そうです。

■ Lucas 数列

講義の後半では Lucas 数列についての紹介がありました。Lucas 数列とは漸化式 $L_{k+2}=PL_{k+1}-QL_k$ によって定義される数列で、初期値 $L_0=0, L_1=1$ で与えられ、P と Q は整数です。$P=1, Q=-1$ とすれば Fibonacci 数列になり、$P=2, Q=-1$ とすると、Pell 数列になるというものです。私が面白いと感じたのは、Lucas 数列を素数を法として計算してみるというものでした。素数を法とした Lucas 数列では、必ず周期性があるというものでした。そして、そこから整数のいろいろな性質を定理として導き出せることを紹介されました。このとき、位数というものが重要な役割を果たしているそうです。このあたりからそろそろ私の理解の範囲を超えてしまいました。

さて、私は講義の途中、Lucas 数列はもしかしたら RSA 暗号と関連があるのでは？と勝手な妄想をしていました。RSA 暗号というのはインターネットのセキュリティ通信で応用されている暗号方式です。この暗号では、素数が重要な役割を果たしています。暗号化においては、巨大な 2 つの素数 $p, q(p \neq q)$ から作る組み合わせ数 $n = pq$ を法としたべき乗計算をします。暗号文の復号化においては、次の性質を利用します。ある数値に対して、n を法として $1, 2, 3, \cdots$ と順次べき乗していくと、$p-1$ と $q-1$ の最小公倍数 ℓ を周期としてもとの数値に戻るという性質です。つまり、任意の数値を n を法として、$m\ell+1(m \in \mathbb{N})$ 乗すれば必ず元の数値に戻るので、簡単に復号することができるのです。

RSA 暗号の暗号文は n を素因数分解をして、p, q を求めることができれば解読できますが、p, q はそれぞれ 300 桁以上の素数なので、スーパーコンピューターを使っても素因数分解には膨大な時間がかかってしまいます。通信ライン上では、n と暗号化のためのべき乗数 e が公開されていますが、素数 p, q は非公開となっています。復号化のための鍵を通信ライン上に送信されないので、通信を途中で傍受しても解読は困難となっています。したがって、RSA 暗号は非常に安全性の高い暗号方式となっています。

さて、講義の内容からだいぶ脱線したようです。講義の内容についていけなくなっていたので、「素数」、「周期性」、「位数」というキーワードから勝手に Lucas 数列と RSA 暗号を関連付けてみた次第です。失礼しました。

■懇親会

最後に懇親会ですが、講義終了後に 20 名ほどの人が参加されました。いつもはここで一人一人の自己紹介を長々とやってしまうのですが、今回は名前と仕事以外は一人一言ということで、非常に手短にそれぞれが自己紹介されました。そのおかげで、みなさんいろいろな人と話す機会があったようです。

私は個人的には諏訪先生とは何年かぶりでお会いして、お話をすることができました。以前は中央大学の特別講義において、社会人がなぜ数学を勉強するのかという内容で、学生の前で講義をさせてもらいました。私にとってはとても貴重な経験でした。

さて、いろいろな人と話をしているうちに、あっという間に懇親会は終了してしまいました。楽しい時間というのは本当に短く感じるものです。

私は現在北海道に住んでおり、なかなか数学工房に顔を出すことは難しいのですが、また機会があればできるだけこのような会に参加したいと思います。最後に諏訪先生、大変興味深い講義をありがとうございました。

写真 2：懇親会の様子

入門桑野道場（第 39 回）

/// 記　桑野道場師範代　半田伊久太 ///

前回の問題

1. $\mathbb{R}^2$ の相異なる 4 点が，どの 2 点間の距離も正整数であるように与えられている．このときどの 2 点間の距離も奇数であることはないことを示せ．
   「33 の素敵な数学小景（イジィ・マトウシェク著　徳重典英訳　日本評論社）」より．
2. V を $\mathbb{R}$ 上の線型空間，$\dim V = n < \infty$ とする．さらに $P : V \to V$ は $\mathbb{R}-$ 線型変換で $P = P^2$ を満たすとする．このとき $\mathrm{rank}P = \mathrm{tr}P$ であることを示せ．
   ただし $\mathrm{tr}P$ は P のトレース（対角和）を表すとする．
3. 【研究問題】 $A := \{1, 2, 3, \ldots, 100\}$（100 以下の正整数全体の集合）と置く．
   A の部分集合 S に対して S の要素の個数を $|S|$ で表すことにする．
   このとき次の命題 $(*)$ を考える．
   「$n\,(1 \leq n \leq 100)$ が与えられたとき，$|S| = n$ を満たす A の任意の部分集合 S に対して以下の条件を満たす $a, b, c, d \in S(a, b, c, d$ は相異なる$)$ が存在する：

   $$a + b = c + d \quad \text{」}$$

   このとき、以下の問に答えよ．
   (a) $n = 16$ のとき命題 $(*)$ は真であることを示せ．
   (b) $n = 13, 14, 15$ のとき命題 $(*)$ は真であるか，偽であるか考察せよ．

解答

1. 距離は平行移動不変だから，1 点を原点，他の相異なる点を a, b, c とする．
もし $\|a\|, \|b\|, \|c\|, \|a-b\|, \|b-c\|, \|c-a\|$ が全て奇数であったとする．余弦定理より，
$2\langle a,b\rangle = \|a\|^2 + \|b\|^2 - \|a-b\|^2\,, 2\langle b,c\rangle = \|b\|^2 + \|c\|^2 - \|b-c\|^2\,, 2\langle c,a\rangle = \|c\|^2 + \|a\|^2 - \|c-a\|^2$
である．ここで $\langle , \rangle$ は内積を表す．明らかに $2\langle a,b\rangle, 2\langle b,c\rangle, 2\langle c,a\rangle$ は整数．ところで $m \in \mathbb{Z}$ が $m \equiv 1 \pmod 2$ ならば $m^2 \equiv 1 \pmod 8$.
すると, 余弦定理の右辺はすべて $1 \pmod 8$ だから, $2\langle a,b\rangle \equiv 2\langle b,c\rangle \equiv 2\langle c,a\rangle \equiv 1 \pmod 8$.
$\pi_8 : \mathbb{Z} \to \mathbb{Z}/8\mathbb{Z}$ を標準写像とし，$\widetilde{\pi}_8 : \mathrm{M}_3(\mathbb{Z}) \ni (a_{ij}) \mapsto (\pi_8(a_{ij})) \in \mathrm{M}_3(\mathbb{Z}/8\mathbb{Z})$ とする．

$$\widetilde{\pi}_8(2\mathrm{G}(a,b,c)) = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix} \quad \text{ここで } \mathrm{G}(a,b,c) \text{ は } a,b,c \text{ のグラム行列を表す．}$$

$$\text{すなわち } \mathrm{G}(a,b,c) = \begin{pmatrix} \langle a,a\rangle & \langle a,b\rangle & \langle a,c\rangle \\ \langle b,a\rangle & \langle b,b\rangle & \langle b,c\rangle \\ \langle c,a\rangle & \langle c,b\rangle & \langle c,c\rangle \end{pmatrix}$$

したがって, $\pi(\det(2\mathrm{G}(a,b,c))) = \det(\widetilde{\pi}_8(2\mathrm{G}(a,b,c))) = 4 \neq 0$．よって, $8 \cdot \det(G(a,b,c)) \neq 0$.
ゆえに $2^3 \cdot \det \mathrm{G}(a,b,c) \neq 0 \Rightarrow \mathrm{G}(a,b,c)$ は正則 $\Rightarrow a,b,c$ は線型独立 $\Rightarrow a,b,c$ は平面ベクトルだから線型従属．これは矛盾．

2. - $v \in \mathrm{Im}P \Leftrightarrow p(v) = v$ であることに注意（容易にわかる）．
- $V = \mathrm{Im}P \oplus \mathrm{Ker}P$ であること．
任意の $v \in V$ に対して，$u_1 := P(v)\,, u_2 := v - u_1$ とおく．$u_1 \in \mathrm{Im}P$ だから $P(u_1) = u_1$ に注意．
$P(u_2) = P(v-u_1) = P(v) - P(u_1) = u_1 - u_1 = \mathbf{0}$.
したがって $u_2 \in \mathrm{Ker}P$．$v = u_1 + u_2$ だから $v \in \mathrm{Im}P + \mathrm{Ker}P$.
よって $V = \mathrm{Im}P + \mathrm{Ker}P$.
$v \in \mathrm{Im}P \cap \mathrm{Ker}P \Rightarrow P(v) = v$ かつ $P(v) = \mathbf{0} \Rightarrow v = \mathbf{0}$.
よって $\mathrm{Im}P \cap \mathrm{Ker}P = \{\mathbf{0}\}$．以上により $V = \mathrm{Im}P \oplus \mathrm{Ker}P$.
- $\mathrm{rank}P = \mathrm{tr}P$ であること．
$\mathrm{Im}P$ の基底を $\{b_1, \ldots, b_r\}$，$\mathrm{Ker}P$ の基底を $\{b_{r+1}, \ldots, b_n\}$ とする．
ここで $1 \leq r \leq n$ である．$B = \{b_1, \ldots, b_n\}$ とおくと B は V の基底で，

$$P(b_j) = \begin{cases} b_j & (1 \leq j \leq r) \\ \mathbf{0} & (r+1 \leq j \leq n) \end{cases}$$

よって V の基底 B による P の行列表示を $[P]_B$ とすると

$$[P]_B = \begin{pmatrix} E_r & \mathbf{O}_{r,n-r} \\ \mathbf{O}_{n-r,r} & \mathbf{O}_{n-r,n-r} \end{pmatrix}. \text{ ここで}$$

E_r は r 次の単位行列，$\mathbf{O}_{p,q}$ は p 行 q 列の零行列を表すものとする．
したがって $\mathrm{rank}P = \mathrm{rank}[P]_B = \mathrm{tr}[P]_B = \mathrm{tr}P = r$.
（トレースは行列表示によらないことに注意）

3.（a）背理法で容易に示すことができる．
（b）$n = 13$ のときの反例は非会員の方ですが以下を教えていただきました．
$\{1, 2, 3, 5, 8, 14, 23, 42, 52, 66, 82, 90, 98\}$

解説

1. 一見どう手をつけてよいかわからない問題ですが，$\mathbb{Z}/8\mathbb{Z}$ に落とし込むことと，グラム行列にもちこむことで鮮やかに解決できます．なおグラム行列の細かい性質については線型代数の本を参照してください．
2. この P はいわゆる射影です．$V = \mathrm{Im}P \oplus \mathrm{Ker}P$ と直和分解して 2 つの空間の基底をとり，行列表示すれば終了です．
3.（a）$n = 16$ の場合は簡単な不等式の評価で出来ます．
（b）$n = 13$ の反例ですが私の力量ではチェックができません．どなたかチェックをお願いします．また $n = 14\,, 15$ の場合はなんともわかっていません．皆様の挑戦をお待ちしております．

今回の問題

1. V：体 K 上の有限次元線型空間，$\dim V = n$ とする．
   U を V の線型部分空間，$U^\circ := \{\varphi \in V^* \,|\, U \subset \mathrm{Ker}\varphi\}$ とおく．
   このとき U° は V^*の線型部分空間で，$\dim U^\circ = n - \dim U$ であることを示せ．
   ここで V^*は V の双対空間，すなわち $V^*= \{\varphi : V \to K \,|\, \varphi$ は $K-$ 線型 $\}$．
2. V, W：体 K 上の有限次元線型空間，$\dim V = n, \dim W = m$ とする．
   $T : V \to W$ を $K-$ 線型写像とするとき，T^*: $W^* \ni \eta \mapsto \eta \circ T \in V^*$で T^*を定義する．このとき次を示せ．
   （a）T^*は $K-$ 線型．（T^*を algebraic adoint と呼ぶ）
   （b）$\mathrm{Ker}T^* = (\mathrm{Im}T)^\circ$かつ $\mathrm{Im}T^* = (\mathrm{Ker}T)^\circ$．
   （c）$\mathcal{A}$ を V の基底，$\mathcal{B}$ を W の基底，$\mathcal{A}^*$を $\mathcal{A}$ の双対基底，$\mathcal{B}^*$を $\mathcal{B}$ の双対基底とする．基底 $\mathcal{A}, \mathcal{B}$ による T の行列表示を $[T]^{\mathcal{B}}_{\mathcal{A}}$，双対基底 $\mathcal{B}^*$, $\mathcal{A}^*$ による T^*の行列表示を $[T^*]^{\mathcal{A}^*}_{\mathcal{B}^*}$ と表すと，$[T^*]^{\mathcal{A}^*}_{\mathcal{B}^*} = {}^t([T]^{\mathcal{B}}_{\mathcal{A}})$ が成立する．ただし行列 A に対して ${}^tA$ は A の転置行列を表す．

問題について一言

2019 年の年始の集中「線型代数」で扱われた問題です．解答お待ちしております．

宛先と締切

宛先　kuwanodojo@googlegroups.com
締切　2019 年 4 月 30 日（火）
(郵送される場合は数学工房オフィスまでお願いいたします)

数学工房　2019 年 2 月 10 日発行
発行人　桑野耕一
編集人　増田卓、坂口尚文、半田伊久太
連絡先
オフィス電話：042-495-6632
数学工房連絡用携帯：080-6576-2691
連絡は極力 e-メールでお願いします。
e-mail：sugakukobo@w5.dion.ne.jp
e-mail：monteverdi2007@ezweb.ne.jp
公式ホームページ
http://www.sugakukobo.com/
数学工房教室
〒170-0003
東京都豊島区駒込 1-40-4
全国蕎麦製粉会館 2F　202・203
数学工房オフィス
〒204-0023
東京都清瀬市竹丘 1-17-26-401